LA-UR-98-4874

Title:

Tamper Detection for Waste Managers

Author(s):

Roger G. Johnston
Anthony R.E. Garcia

Submitted to:

http://lib-www.lanl.gov/la-pubs/00418763.pdf

Los Alamos
NATIONAL LABORATORY

Los Alamos National Laboratory, an affirmative action/equal opportunity employer, is operated by the University of California for the U.S. Department of Energy under contract W-7405-ENG-36. By acceptance of this article, the publisher recognizes that the U.S. Government retains a nonexclusive, royalty-free license to publish or reproduce the published form of this contribution, or to allow others to do so, for U.S. Government purposes. The Los Alamos National Laboratory requests that the publisher identify this article as work performed under the auspices of the U.S. Department of Energy. Los Alamos National Laboratory strongly supports academic freedom and a researcher's right to publish; therefore, the Laboratory as an institution does not endorse the viewpoint of a publication or guarantee its technical correctness.

Tamper Detection for Waste Managers

Roger G. Johnston and Anthony R.E. Garcia

Vulnerability Assessment Team
Los Alamos National Laboratory
MS J565, Los Alamos, NM 87545

ABSTRACT

Tags and seals have an important role to play in waste management. They can be used for hazardous materials accountability and control. They can help detect tampering, theft, sabotage, or errors in handling and processing. The Vulnerability Assessment Team at Los Alamos National Laboratory has extensively analyzed tags and seals, as well as a number of tamper-detection security programs. As a result of this work, we have developed suggestions for choosing and using tags and seals, and for effective tamper detection. This paper covers suggestions that are the most relevant for waste management applications.

INTRODUCTION

Tags, tamper-indicating seals, and tamper-evident packaging have an important role to play in the management, transport, and storage of hazardous waste [1,2]. They can aid in material accountability and control, verification, nonproliferation, counter-terrorism, security and safeguards, and reducing legal liability. They can help to protect against inadvertent errors in storage and handling, malicious tampering or theft, and unscrupulous efforts to dispose of hazardous waste in containers already certified to contain non- or less hazardous waste. Tags and seals can also help to protect against tampering with waste data, analysis results, and analytical instruments.

The Vulnerability Assessment Team (VAT) at Los Alamos National Laboratory [2,3] has analyzed over 110 different tags and seals, both government and commercial [4,5]. The Team has performed vulnerability assessments and provided assistance with tamper detection for a dozen government agencies and ten private companies. We have also developed detailed training curriculum for seal installers and inspectors. As a result of these activities, the VAT has compiled a number of lessons and suggestions for tamper detection. We believe some of these generic recommendations can help waste managers choose appropriate tags and seals, and use them with maximum efficiency and effectiveness.

In this paper, we mostly focus on seals. The effective use of seals is probably of greater importance to most waste managers than concentrating on tags or locks. Many waste processing facilities already have effective ways to mark waste storage containers. Many have effective physical security to delay and deter unauthorized access to the facility. Such access control may include fencing, intrusion alarms, security guards, ID badges, biometrics, and locks. Seals, however, offer the possibility of inexpensively protecting against deliberate or accidental tampering by both insiders and outsiders.

TAMPER DETECTION TERMINOLOGY & CONCEPTS

There is a great deal of confusion, even among experienced security professionals, about the definitions, roles, and functions of various security devices. It is not always clear to even experts which security devices are most appropriate for a given application, or how they should be used for greatest effect. The following mini-glossary may be useful for clarifying tamper detection issues.

lock: hardware designed to delay and complicate unauthorized entry or access. Locks do not stop adversaries who are adequately motivated and/or knowledgeable.

safe: a container that serves the function of a lock. It may also be designed to prevent damage to contents during a fire.

vault: a room-sized safe.

seal: a device or material designed to leave unerasable evidence of unauthorized access. Seals often provide little resistance to unauthorized entry--they simply record that it took place.

security seal: a seal.

tamper-indicating seal: a seal.

antipilferage seal: a seal used primarily to detect (or possibly discourage) theft.

tamper-indicating device (TID): a seal.

barrier seal: a hybrid security product that serves as both a lock and a seal.

passive seal: a seal that works without electrical power, either battery or externally generated. Passive seals are usually not reusable.

active or dynamic seal: a seal that is routinely powered by electricity (internally or externally). Active seals are often reusable.

intrusion or burglar alarm: an active seal that reports unauthorized entry or access in real-time.

tamper-evident packaging: the packaging or the container incorporates tamper-indicating seal(s).

tampering: Gaining unauthorized access to an object, data, paperwork, or the contents of a container or room. This may be for the purposes of stealing, copying, changing, supplementing, corrupting, scrambling, sabotaging, contaminating, spoiling, hacking, damaging, disrupting, or simply looking at the item(s) of interest.

tag: an intrinsic or applied unique characteristic (“fingerprint”) used to unambiguously identify an object or container.

defeating a seal: gaining entry or access through the seal to what the seal is protecting without being detected.

defeating a tag: counterfeiting it, or removing it from one object and placing it on another without being detected.

attacking a tag or seal: trying to defeat it.

compromising or spoofing a tag or seal: defeating it.

vulnerability assessment: finding (and often demonstrating) the weaknesses in a security device or security program, often accompanied by suggested counter-measures.

Note that classifying a security device as a tag, seal, or lock is complicated by the fact that most devices have some attributes of each. A lock may reveal evidence of unauthorized entry if it has been attacked with brute force. Some seals, such as those commonly used for cargo security, are designed to be hybrid products--part lock and part seal. Such “barrier seals” are a compromise; they usually perform neither function optimally. Seals may also be used as tags because--at least in theory--any attempt to remove a seal and place it on another object will be recorded by the seal as tampering. Indeed to be effective, a seal must possess some kind of tag-like identifier, i.e., a novel characteristic or unique “fingerprint”, such as a serial number. Otherwise, an adversary can simply remove the original seal and replace it with an exact duplicate. Tags, in turn, are sometimes used as seals since they must record any effort to remove them. To further complicate matters, many active seals such as fiber optic or electronic seals often play the role of an intrusion alarm.

TYPES OF SEALS

Ancient Seals

Seals were in use before the invention of writing. A typical ancient seal consisted of a small cylinder or stamp made of clay, wood, stone, or bone, and carved with a complex design. Various containers such as pots, jugs, or baskets were secured by placing clay over the lid, mouth, cap, or stopper. The stamp or cylinder seal was then used to impress a pattern into the clay, either by pressing the stamp seal, or by rolling the cylinder seal along the clay. The clay was allowed to harden, perhaps by baking in the sun. Any attempt to open the container would presumably require fracturing the clay. Replicating the pattern to reseal the container (and hide the fact that it had been opened) would require significant time and skill if the trespasser did not possess the original seal. Alternatively, a cord could be tied around a container or package, and a bulla (lump of clay) placed around the knot, prior to pressing the seal design into the clay.

Another ancient use for seals was for documents. Written clay tablets from 5000 B.C. onward were often imprinted with the design from a stamp or cylinder seal. This was intended to be a tag-like signature to authenticate the document and identify the author. The clay tablet might also be sealed inside a clay envelope to prevent tampering. The envelope was also frequently imprinted with a seal design.

The Egyptians were using bullae to seal papyrus documents shortly after 3000 B.C. They also used seals on the tombs of their dead. When the burial chamber was completed and the mummified body placed inside, the door was sealed with mud and plaster. The door could still be opened, but it would then be obvious that the seal was broken. In modern times, archaeologists were able to tell if a tomb had been looted by checking to see if the seal was intact.

From 1100 BC through medieval times, wax seals were widely used in Europe. Wax was melted and then dripped onto a scroll. (Shellac eventually replaced wax.) A signet ring--engraved with a distinctive design--was then pressed into the molten blob of wax, leaving behind the complex design.

Modern Seals

There are at least several thousand different commercial seals available. References 1 and 6 discuss them in more detail. A variety of different kinds of seals are shown in figure 1.

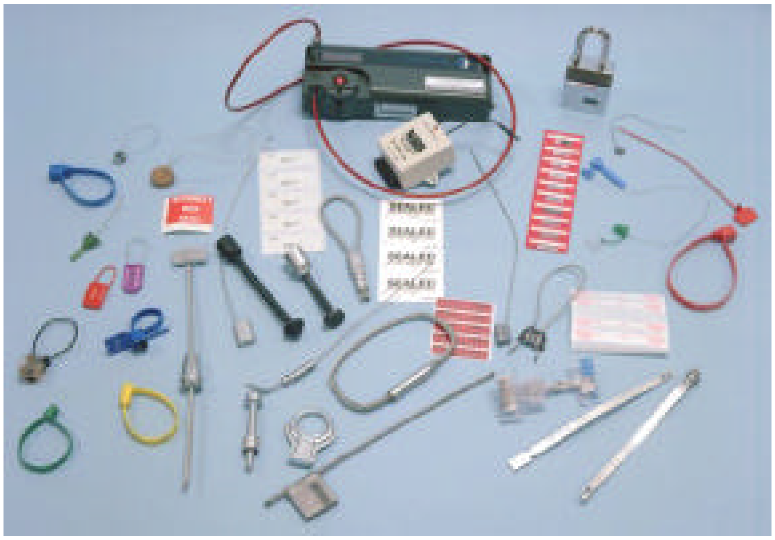

Figure 1 - Just a few of the many available commercial seals.

Modern seals can be categorized as passive or active (also called “dynamic”). The first eleven seal types discussed below are passive. The last two are active.

wire loop seal: This seal consists of one wire twisted around one or more wires. The wire bundle is then passed through the hasp of a container or door. A metal or plastic head or housing then crimps, traps, or irreversibly captures the ends of the wire bundle. See figure 2. The lead-wire seal is the classic example of this type of seal. A blob of soft lead is used to crimp the ends of the wire bundle. Lead-wire seals, however, have fallen out of favor because of the poor security they offer and because of the health and environmental problems presented by lead.

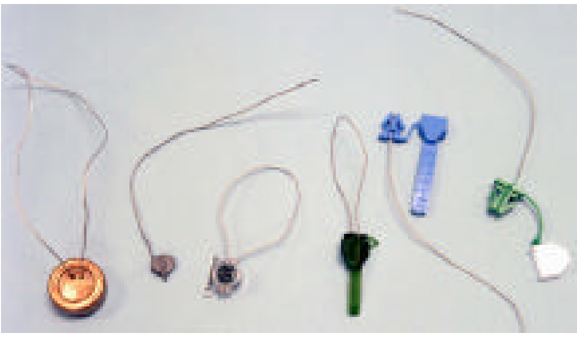

Figure 2 - Examples of wire loop seals. The seal second from the left is a traditional lead-wire seal.

metal cable seal: A larger and sturdier version of the wire loop seal. Aircraft cable is used with each end crimped or irreversibly clamped into a head or housing. Because of its great resistance to force, this is a barrier seal--part lock and part seal.

plastic strap or ribbon seal: A one-piece plastic molded strap with one end that snaps irreversibly into a head or housing on the other end, after the plastic strap is passed through the hasp of a container or door. Typically very inexpensive. Examples are shown in figure 3.

metal ribbon (car-box or car-ball) seal: A seal made from sheet metal. See figure 3. One end of the ribbon snaps irreversibly into a head on the other end. Popular for use on railcars. More robust than a plastic strap seal, though still not considered a barrier seal.

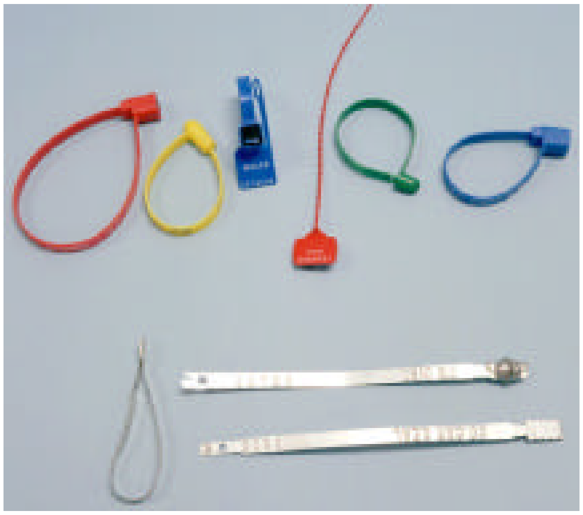

Figure 3 - Some plastic strap seals (top) and metal ribbon seals (bottom).

bolt seal: A strong bolt with one end larger than the hasp and the other end designed to snap irreversibly into a cylindrical head or housing called the “locking head” or “locking body”. These barrier seals are popular for use on trucks and transportainers. Bolt seals can usually withstand substantial force without opening.

padlock seal: A “self-locking” metal or plastic seal that looks like a padlock. Intended for one-time use. Despite the name, these seals are usually not meant to function as locks. Often used on residential and commercial utility meters.

adhesive tape seal (adhesive label or pressure-sensitive adhesive seal): Sticky labels that are damaged if removed from what they are stuck to. See figure 4. Often used as tags.

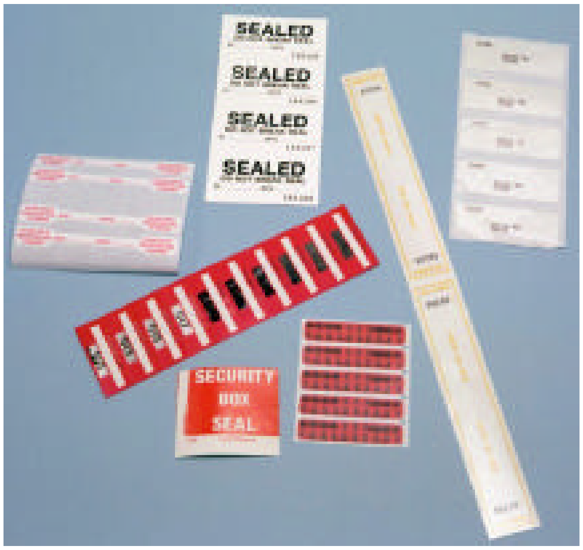

Figure 4 - Just a few of the hundreds of commercially available pressure-sensitive adhesive seals.

tamper-evident packaging: includes frangible foils, brittle films, plastic wrap, pop-up pressure bubbles, and break-off caps, lids, or tabs designed to indicate if the package has been opened. Often used on consumer products. Tamper-evident packaging is now required on all over-the-counter pharmaceuticals sold in the United States.

secure container: The tamper-indicating equivalent of a safe. The container is the seal.

security clamp: A device designed to show or cause damage if a door, panel, window, or other opening is used for entry.

(passive) fiber optic seal: The cable is an optical fiber or bundle of optical fibers. Cutting the optical fibers changes their light transmission or other properties.

(active) fiber optic seal: In an active fiber optic seal, light pulses are sent down the optical fibers many times per second. If the optical fibers are cut, the light pulses fail to complete the loop and this is detected by electrooptics.

(active) electronic seal: Seals of this sort are usually battery powered and check continuously for signs of tampering. This type of device is often as much an intrusion (burglar) alarm as a seal. If the device uses active fiber optics, it is usually classified under that category.

SUGGESTIONS FOR TAG & SEAL USERS AND POTENTIAL USERS

We can offer a number of generic recommendations for tag and seal users (or potential users) based on our experiences with tamper detection, tag/seal vulnerability assessment, and the review of various security programs. Not every one of these suggestions is automatically appropriate for any given security/verification program, nor necessarily lacking. It is our view nevertheless that most programs would benefit from implementing at least some of these suggestions.

(1) Many users of tags and seals are remarkably vague on what they are trying to accomplish. It is essential to fully understand the goals of the security or verification program, the resources available, the required functions of the tags and seals, what is being protected and why, the consequences of a security failure, and the nature of potential adversaries and the resources they have at their disposal. Security and reliability cannot be optimized without a clear understanding of these issues. These matters should be revisited on a regular basis.

(2) In choosing a tag or seal, bear in mind that the unit cost is often the least important economic factor. Costs associated with installation, inspection, and training are often more significant.

(3) Factors in addition to security and economics deserve particular attention in choosing a tag or seal for waste management applications. These include ease of use, robustness, durability, and safety. Ease of use may be critical if the tags or seals must be installed, inspected, and removed under inclement weather conditions or poor lighting, or while wearing chemical protective gear. Robustness may be an important issue for tags or seals used on waste containers that can potentially receive rough handling. Environmental durability can be very important if the tags or seals are to be used, for example, on waste drums stored out of doors. Many commercial plastic seals are doped with compounds to protect them from ultraviolet damage caused by sunlight. Certain metal seals may not be good choices for use in a salt-air environment (such as near the ocean) because of the potential for corrosion. Extreme temperature ranges may also eliminate the use of certain tags or seals. Safety can be an important issue as well, particularly for wire-loop, metal cable, and metal ribbon seals. If they are attached to waste containers such as 55-gallon drums that are moved frequently, there is the possibility of catching fingers in the loops, or gouging the skin, eyes, or protective clothing of waste workers.

(4) There should be periodic, effective vulnerability assessments of both the tags/seals being used and the overall security or verification program. Reference 7 discusses the attributes of effective vulnerability assessments.

(5) Always bear in mind that ALL security devices and ALL security programs can be defeated by a motivated adversary--often quickly and remarkably easily. Assurances from manufacturers, vendors, and security personnel that their products or security programs are “tamper-proof” should be vehemently ignored. Effective security is never compatible with over-confidence!

(6) Vendors, developers, and manufacturers of tags and seals often emphasize how difficult it is to counterfeit their products. Potential users should be wary of this; the degree of

difficulty is often exaggerated. In addition, counterfeiting is usually one of the least likely attack scenarios for most tags and seals. Other attack methods are usually easier to implement.

(7) Tags and seals should be viewed as only one part of an overall security or verification program. Discovering vulnerabilities in a tag or seal does not necessarily mean that the entire security/verification program has failed. On the other hand, users of tags and seals should not overlook opportunities to optimize tag/seal security--especially since this can usually be done in a simple, cost-effective manner.

(8) Loop-type seals that are adjustable should be cinched as tightly against the container hasp as practical. This often contradicts the instructions given by seal manufacturers. It may also complicate the tasks of inspecting and removing the seal. Tight cinching, however, complicates seal attacks and increases the odds of detecting them. It also improves safety.

(9) Tags and seals must be inspected if tampering is to be detected. Unlike locks, they do not provide security if ignored. Sometimes inspection is done using electronic or optical readers, or computers. Most tags and seals, however, are still inspected manually and visually. Tag and seal inspectors, we believe, must be familiar with the most likely attack scenarios associated with the tag/seal they are using, and specifically look or test for them. Most manufacturers of tags and seals provide little useful information on how to inspect a tag or seal. Vague instructions to, for example, "look for signs of tampering" are not satisfactory. Tag/seal inspectors should be shown examples of defeated tags and seals so they know exactly what to look for in the specific tag or seal they are using. This suggestion is somewhat controversial in that many security managers are reluctant to disseminate vulnerability information to relatively low-level personnel. In our view, if tag/seal inspectors are too untrustworthy to be given such information, the security or verification program probably has more serious problems than simply tag and seal vulnerability.

(10) Tags or seals that are inspected visually should be examined with an identical, unused tag or seal held right alongside. People do not accurately remember details of exact color, size, surface texture, gloss, and patterns, but they are usually very proficient at visual side-by-side comparisons. Counterfeits can be more reliably spotted in this way.

(11) Inspectors should be rewarded, not punished, for finding potential problems, raising important issues, and thinking on the job. In many security programs, inspectors are afraid to raise concerns about suspicious tags/seals or questionable procedures because of the consternation this causes their supervisor.

(12) To the extent practical, personnel involved with tags and seals should be emotionally and intellectually engaged in the security/verification task. Inspectors should fully understand the reasoning behind the inspection process; they should not be mindlessly following an overly formal inspection protocol.

(13) Most users of tags and seals are careful about protecting the devices prior to use. Tags

and seals, however, must also be thoroughly protected or destroyed after use. Discarded tags and seals, even if partially destroyed, provide potential adversaries with a useful source of information, practice samples, and counterfeit parts.

(14) If practical, used tags and seals should be archived for possible future analysis as new attacks are uncovered, or issues of past vulnerability arise.

(15) Tag or seal data must be very well protected. Information about a tag or seal, such as the serial number, must not be stored in or on the container being protected, unless the information is appropriately encrypted. The driver of a sealed truck should not possess the working copy of paperwork containing the seal serial number. Seal data that is communicated, shipped, or carried to another location must be secure.

(16) Manufacturers should not sell or provide free samples of seals lacking serial numbers. These are an excellent source for counterfeiting. Free samples should be a different color from the commercial product, or be blatantly marked in some other fashion.

(17) In our experience, assurances from vendors and manufacturers that they will protect seal logos or certain serial numbers from unauthorized users are not always reliable. This should be covertly tested by the tag/seal customer.

(18) (Ideally the same) serial number should appear on every independent part of a seal. If serial numbers are stamped or embossed on a tag/seal by the manufacturer, they should be done deeply enough that they can’t be easily buffed off.

(19) It is important to keep in mind that simple physical attacks on high-tech systems, products, or security/verification programs are often highly effective because of the ease with which they can be accomplished, and because users and developers of high-technology systems often focus on other issues [8].

(20) Blink comparators [2, 9] are highly effective for comparing “before” and “after” images of a tag or seal for evidence of change. They usually out-perform complex readers and computer pattern recognition algorithms. The commonly used correlation coefficient, for example, is a particularly poor algorithm for many such image comparisons [10].

(21) Tags and seals based on adhesive labels do not, in our view, provide high levels of security. They often have limited robustness and environmental durability as well. If they are to be used, they should be protected for the first 48 hours after application, because of incomplete adhesion. (Heat can help speed up the process.) Users should clean the surface prior to application, and watch for surfaces that may have been pre-oiled or pre-coated to reduce adhesion. The adhesive, printing ink, and label substrate should be soluble in exactly the same solvents. The adhesive should melt at a higher temperature than the printing inks and substrate. Inspectors should examine not just the label, but the general area around the label. They should also pay particular attention to areas on the label that have not adhered to the surface, such as over slots, grooves, or screw holes. Labels should be compared side-by-side with an unused label.

CONCLUDING REMARKS

Tags and seals can be of considerable value for waste management applications. It is important, however, that they be chosen appropriately and used in a manner that optimizes their security. Like all security devices, tags and seals are only as good as the security program and the personnel that use them. Tags and seals that are used mindlessly or without paying close attention, or that are slapped in place and then forgotten, will not provide effective security. Indeed, they may be less than worthless if they create a naive over-confidence in the mind of the user.

The suggestions offered in this paper are generic. Because the best suggestions for effective tamper detection are highly application and hardware specific, tag and seal users may benefit from specific advice. Legitimate users or potential users of tags and seals are welcome to contact the Vulnerability Assessment Team at Los Alamos National Laboratory to discuss tamper detection issues.

ACKNOWLEDGMENTS

This work was performed under the auspices of the United States Department of Energy. We benefited from the assistance of Eric Baca, Ron Martinez, and Anna Nogar.

REFERENCES

1. G. STAEHLE (Editor), “Verification Technologies: DOE's Tags and Seals Program”, DOE Report DP/OAC/VT-92B, Washington, D.C. (1992).

2. R.G. JOHNSTON, "The Real Deal on Seals", Security Management 41, 93 (1997).

3. Y. ONO, “Now, Los Alamos Proves It Can Open a Bottle of Aspirin”, Wall Street Journal, page A1, March 13, 1997.

4. R.G. JOHNSTON, A.R.E. GARCIA, and W.K. GRACE, "Vulnerability Assessment of Passive Tamper-Indicating Seals", Journal of Nuclear Materials Management 224, 24 (1995).

5. R.G. JOHNSTON and A.R.E. GARCIA, "Vulnerability Assessment of Security Seals", Journal of Security Administration 20, 15 (1997).

6. “DoD Antipilferage Seal User’s Guide”, Naval Facilities Engineering Service Center, Port Hueneme, CA (1997).

7. R.G. JOHNSTON, "Effective Vulnerability Assessment of Tamper-Indicating Seals", Journal of Testing and Evaluation 25, 451 (1997).

8. R.G. JOHNSTON and A.R.E. GARCIA, "Physical Security and Tamper-Indicating Devices", Proceedings of the American Society of Information Science Mid-Year 1997 Meeting, Scottsdale, AZ, pp. 43-46 (1997).

9. H.E. LAZERSON, “Blink Comparator”, Arch. Ophth. 102, 635 (1984).

10. E.K. YEN and R.G. JOHNSTON, "The Ineffectiveness of the Correlation Coefficient for Image Comparisons", Report LAUR-96-2474, Los Alamos National Laboratory (1996).